

McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 13, 2025

VIA U.S. MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: E-Benefit Solution – Incident Notification

McDonald Hopkins PLC represents E-Benefit Solution (“E-Benefit”). I am writing to provide notification of an incident at E-Benefit that may affect the security of personal information of approximately eighty-five (85) Maryland residents. By providing this notice, E-Benefit does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

E-Benefit recently became aware of unauthorized access to its network environment. Upon learning of the issue, E-Benefit launched an investigation, contained and secured the network, eradicated the threat and alerted law enforcement. As part of the investigation, E-Benefit has been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. The investigation aimed to determine the nature and scope of the incident and whether any sensitive data, including personal information was accessed and/or acquired by the unauthorized party. After a thorough and detailed forensic investigation, E-Benefit discovered on December 10, 2024 that the unauthorized actor accessed the network and removed certain files containing personal information from its network environment on July 11, 2024. The information included residents’ full names, Social Security number, health insurance policy number, government ID number, and protected health information. Please note that impacted elements vary by individual.

E-Benefit is not aware of any reports of identity fraud or improper use of any personal or protected health information as a direct result of this incident. Nevertheless, E-Benefit wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. E-Benefit is providing the affected residents with written notification of this incident commencing on or about January 13, 2025 in

substantially the same form as the letter attached hereto. E-Benefit is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents whose Social Security numbers were impacted are being offered complimentary credit monitoring for one year. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At E-Benefit, protecting the privacy of personal information is a top priority. E-Benefit is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. E-Benefit continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (312)-642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'BLD', with a long horizontal flourish extending to the right.

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to E-Benefit Solution ("E-Benefit"). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved some of your personal information. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

E-Benefit recently became aware of unauthorized access to our network environment.

What We Are Doing

As soon as we became aware of the issue, we launched an investigation, contained and secured the network, eradicated the threat and alerted law enforcement. As part of the investigation, we have been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. The investigation aimed to determine the nature and scope of the incident and whether any sensitive data, including personal and/or health information, was accessed and/or acquired by the unauthorized party.

After a thorough and detailed forensic investigation, we determined the unauthorized actor accessed our network and, as a result, removed and accessed certain files from our network environment. Upon learning this, we promptly conducted an extensive and comprehensive review of the impacted files and, on December 10, 2024, we discovered that certain files containing your personal information may have been accessed and/or acquired by the unauthorized party.

What Information Was Involved?

The data involved contained some of your personal information, including your full name and [REDACTED]

What You Can Do

To date, we are not aware of any reports of identity fraud or identity theft as a direct result of this incident. Nevertheless, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include [REDACTED] months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information. For more information and instructions on how to activate your complimentary credit monitoring membership, please review the "Other Important Information" section.

For More Information

E-Benefit values your privacy and deeply regrets that this incident has occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [REDACTED].

This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, [REDACTED] p.m. Eastern Time, excluding holidays.

Sincerely,

E-Benefit Solution

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary [REDACTED] month Credit Monitoring.

A. Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

B. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
m
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
[http://www.transunion.com/securityfre](http://www.transunion.com/securityfreeze)
eze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal

identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits” statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC

20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

* * * * *

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a

victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

* * * * *

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

